CLAIMS:

1. A method comprising:

establishing a packet tunnel having a source network address and a destination network address;

detecting a network attack;

selecting a new network address for at least one of the source network address and the destination network address upon detecting the network attack; and

establishing a new packet tunnel using the new network address.

2. The method of claim 1, wherein the source network address and the destination network address comprise port numbers.

3. The method of claim 1, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses.

4. The method of claim 1, wherein detecting a network attack comprises detecting an attack on an access link coupling the destination network device to the network.

5. The method of claim 1, further comprising:

reserving for the packet tunnel an amount of bandwidth within an access link coupled to a destination network device that terminates the packet tunnel;

upon detecting the network attack, canceling the reserved bandwidth for the packet tunnel; and

reserving for the new packet tunnel an amount of bandwidth within the access link.

6. The method of claim 1, further comprising exchanging a set of available network addresses between a source network device originating the packet tunnel and a destination network device terminating the packet tunnel.

7. The method of claim 1, further comprising:

maintaining a set of available network addresses;

selecting one of the network addresses as the new network address;

establishing a new packet tunnel using the new network address for the destination address; and

reserving for the new packet tunnel an amount of bandwidth within an access link.

8. The method of claim 1, wherein establishing a new packet tunnel using the new network address further comprises:

selecting an intermediate network device;

establishing a first packet tunnel that terminates on the intermediate network device; and

establishing a second packet tunnel that originates from the intermediate network.

9. The method of claim 8, further comprising:

sending a message from a destination network device to a source network device instructing the source network device to establish the first packet tunnel with the intermediate network device; and

reserving for the second packet tunnel an amount of bandwidth within an access link coupling the destination network device to the network.

10. The method of claim 9, further comprising:

establishing a secure signaling channel between the source network device and the destination network device; and

sending the message via the secure signaling channel.

11. The method of claim 8, further comprising

de-encapsulating at the intermediate network device packets received from the first packet tunnel; and

re-encapsulating the packets at the intermediate network device for communication via the second packet tunnel.

12. The method of claim 8, further comprising:

establishing a secure signaling channel between a source network device and a destination network device;

sending via the secure signaling channel control packets between the source network device and the destination network device to monitor the performance of the first and second packet tunnels; and

selecting a new intermediate network device when the performance reaches a minimum threshold.

13. The method of claim 12, further comprising maintaining a set of possible intermediate network devices, and wherein selecting the intermediate network device comprises selecting one of the possible intermediate network devices from the set.

14. The method of claim 5, wherein reserving an amount of bandwidth comprises sending a reservation message from a destination network device terminating the packet tunnel to a service provider access device.

15. The method of claim 14, wherein sending a reservation message comprises sending the reservation message according to the Resource Reservation Protocol (RSVP).

16. The method of claim 1, wherein establishing a packet tunnel comprises:
maintaining a set of available multicast network addresses;
selecting one of the multicast network addresses for the packet tunnel; and
subscribing to a multicast channel for the selected multicast network address.

17. The method of claim 16, wherein establishing a new packet tunnel comprises:
unsubscribing to the multicast channel;
selecting one of the multicast network addresses for the destination network address;
establishing a new packet tunnel using the new destination address; and
subscribing to a multicast channel for the selected multicast network address.

18. A method comprising:

establishing a packet tunnel having a source network address and a destination network address; and

establishing for the packet tunnel a truncated reservation path within an access link coupled to a destination network device that terminates the packet tunnel.

19. The method of claim 18, wherein the source network address and the destination network address comprise port numbers.

20. The method of claim 18, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses.

21. The method of claim 18, wherein establishing a truncated reservation path comprises issuing a reservation command from the destination device to reserve an amount of bandwidth within the access link for the packet tunnel.

22. The method of claim 18, further comprising:

detecting a network attack; and

canceling the truncated reservation path for the packet tunnel upon detecting the network attack.

23. The method of claim 22, further comprising:

establishing a new packet tunnel upon detecting the network attack; and.

reserving for the new packet tunnel an amount of bandwidth within the access link.

24. The method of claim 18, wherein establishing a truncated reservation path comprises sending a reservation message from a destination network device terminating the packet tunnel to a service provider access device coupled to the destination network device via an access link, wherein the reservation message indicates that packet flow for the tunnel terminates with the destination device.

25. The method of claim 24, wherein sending a reservation message comprises sending the reservation message according to the Resource Reservation Protocol (RSVP).

26. The method of claim 18, wherein detecting a network attack comprises detecting an attack on an access link coupling the destination network device to the network.

27. A method comprising:

establishing virtual private network service including a packet tunnel having a source network address and a destination network address;

detecting a network attack; and

establishing new virtual private network service upon detecting the network attack, wherein the new virtual private network service comprises two or more concatenated packet tunnels.

28. The method of claim 27, wherein establishing the new virtual private network service comprises:

selecting an intermediate network device upon detecting the network attack;

establishing a first packet tunnel from the source network address and terminating on the intermediate network device; and

establishing a second packet tunnel originating from the intermediate network device and terminating at the destination network address.

29. The method of claim 27, wherein establishing a packet tunnel comprises:

maintaining a set of available multicast network addresses;

selecting one of the multicast network addresses for the destination network address of the packet tunnel; and

subscribing to a multicast channel for the selected multicast network address.

30. The method of claim 27, wherein detecting a network attack comprises detecting an attack on an access link coupling the destination network device to the network.

31. A method comprising:

maintaining a set of alternate multicast network addresses and a set of alternate unicast network addresses;

assigning one of the multicast network addresses to a packet tunnel terminating on a network device; and

assigning one of the unicast network addresses to a packet tunnel originating from the network device.

32. The method of claim 31, further comprising:

detecting a network attack; and

selecting a new multicast network address for the packet tunnel terminating on the network device upon detecting the network attack.

33. The method of claim 31, further comprising subscribing to a multicast channel for the multicast network address assigned to the packet tunnel terminating on the network device.

34. The method of claim 33, further comprising:

detecting a network attack;

unsubscribing to the multicast channel;

selecting a new multicast network address for the packet tunnel terminating on the network device upon detecting the network attack; and

subscribing to a new multicast channel for the new multicast network address.

35. A system comprising

a source device coupled to a network; and

a destination device coupled to the network, wherein the source device and the destination device establish a packet tunnel having a source network address and a destination network address and, upon detecting a network attack, select a new network address for at least one of the source network address and the destination network address and establish a new packet tunnel.

36. The system of claim 35, wherein the source network address and the destination network address comprise port numbers.

37. The system of claim 35, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses.

38. The system of claim 35, wherein the destination device and the network device comprise edge routers that couple local area networks to the network.

39. The system of claim 35, wherein the destination device detects an attack on an access link coupling the destination network device to the network

40. The system of claim 35, wherein the destination device reserves for the packet tunnel an amount of bandwidth within an access link coupling the destination network device to the network, and further wherein upon detecting the network attack the destination device cancels the reserved bandwidth for the packet tunnel and reserves the bandwidth for the new packet tunnel.

41. The system of claim 35, wherein the destination device and the source device exchange a set of available network addresses for the source network address and the destination network address of the packet tunnel.

42. The system of claim 35, wherein the destination device comprises a storage medium to store a set of available network addresses for use as the source network address and the destination network address of the packet tunnel.

43. The system of claim 35, wherein the source device and destination device establish the packet tunnel by establishing a first packet tunnel that terminates on an intermediate network device, and establishing a second packet tunnel that originates from the intermediate network.

44. The system of claim 43, wherein the intermediate network device de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination device via the second packet tunnel.

45. The system of claim 43, wherein the source device and the destination device establish a secure signaling channel and send via the secure signaling channel control packets to monitor the performance of the first and second packet tunnels.

46. The system of claim 45, wherein the destination device selects a new intermediate network device when the performance reaches a minimum threshold.

47. A system comprising

a source device coupled to a network by a first access link, wherein the source device originates a packet tunnel; and

a destination device coupled to the network by a second access link, wherein the destination device terminates the packet tunnel, and further wherein the destination device establishes for the packet tunnel a truncated reservation path within the second access link.

48. The system of claim 47, wherein the destination device issues a reservation command to a service provider device to reserve an amount of bandwidth within the second access link.

49. The system of claim 47, wherein the destination device cancels the truncated reservation path upon detecting a network attack.

50. The system of claim 49, wherein the destination device establishes a new packet tunnel upon detecting the network attack and reserves for the new packet tunnel an amount of bandwidth within the second access link.

51. A system comprising:

a source network device that originates a first packet tunnel;

an intermediate network device that terminates the first packet tunnel and originates a second packet tunnel; and

a destination network device that terminates the second packet tunnel, wherein the intermediate network device de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination device via the second packet tunnel.

52. The system of claim 51, wherein the destination network device includes a storage medium to store a set of possible intermediate network devices, and further wherein the destination network device selects the intermediate network device from the set upon detecting a network attack.

53. A computer-readable medium comprising instructions to cause a processor to:

establish a packet tunnel having a source network address and a destination network address;

detect a network attack;

select a new network address for at least one of the source network address and the destination network address upon detecting the network attack; and

establish a new packet tunnel using the new network address.

54. The computer-readable medium of claim 53, further comprising instructions to cause the processor to:

reserve for the packet tunnel an amount of bandwidth within an access link;

upon detecting the network attack, cancel the reserved bandwidth for the packet tunnel; and

reserve an amount of bandwidth for the new packet tunnel.

55. The computer-readable medium of claim 53, further comprising instructions to cause the processor to:

maintain a set of available network addresses;

select one of the network addresses as the new network address;

establish a new packet tunnel using the new network address for the destination address; and

reserve for the new packet tunnel an amount of bandwidth within an access link.

56. The computer-readable medium of claim 53, further comprising instructions to cause the processor to:

select an intermediate network device;

establish a first packet tunnel that terminates on the intermediate network device; and

establish a second packet tunnel that originates from the intermediate network.